UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/805,279	03/13/2001	Robert M. Barnhart	SAIC0039	1264

75131 7590 01/29/2008

KING & SPALDING LLP (SAIC CUSTOMER NUMBER)
ATTN: GEORGE T. MARCOU
1700 PENNSYLVANIA AVE, NW
SUITE 200
WASHINGTON, DC 20006

EXAMINER	
JARRETT, SCOTT L	

ART UNIT	PAPER NUMBER
3623	

MAIL DATE	DELIVERY MODE
01/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/805,279	BARNHART, ROBERT M.	
	Examiner	Art Unit	
	SCOTT L. JARRETT	3623	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 December 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *29-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *29-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 December 2007* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Non-Final Office Action is in response to Applicant's amendment filed December 13, 2007. Applicant's amendment amended claims 29-33. Currently Claims 29-33 are pending.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on December 13, 2007 has been entered.

Response to Amendment

3. The Objection to Claims 31 and 32 in the previous office action is withdrawn in response to Applicant's amendments to Claims 31 and 32.

The Objection to Figure 3B is withdrawn in response to Applicant's amendments to Figure 3B.

The Objection to Figure 5 in the previous office action is not withdrawn.

The Objection to the Specification in the previous office action is not withdrawn.

Response to Arguments

4. Applicant's arguments filed s December 13, 2007 have been fully considered but they are not persuasive. Specifically Applicant's argue that:

a) the new (replacement) Figure 5 is not new matter, and as already been entered (Bullet 1, Page 6);

b) the deletion from the SUMMARY OF THE INVENTION of unclaimed subject matter does not amount to introduction of new matter (Bullets 2-3, Page 6; Last Two Paragraphs, Page 7; Page 8; Paragraph 1, Page 9);

c) the OA makes a mistake of fact in asserting that the original specification does not disclose individual verifiability (Last Bullet, page 6);

d) the recent OA mischaracterizes SHRADER and CRANOR with the effect that the claims as submitted by the applicant, have not yet been examined. Mischaracterized terms include "cast ballots," "vote serial number," and "user.", Bullet 1, Page 7);

e) SHRADER discloses the wrong data, encrypted with the wrong key (Bullet 2, Page 7);

f) the recent OA mischaracterizes SHRADER and CRANOR to find a non-existent "user" in those references." (Bullet 3, Page 7)

g) the recent OA mischaracterizes SHRADER to find a claimed comparison (Bullet 4, Page 7)

h) the recent OA neglects to account for an Element of the Confirmation Token (Bullet 5, Page 7)

a) In response to Applicant argument that the new (replacement) Figure 5 is not new matter, and as already been entered (Bullet 1, Page 6), the examiner respectfully disagrees.

Applicant's is correct Figure 5 was entered as part of the office action mailed March 2, 2006 in response to the Applicant's submission of replacement drawings for all the figures in the instant application; however Figure 5 was inadvertently entered by the examiner. Specifically Figure 5 includes new matter wherein the examiner has been unable to find any support, in the paragraphs cited by the applicant's or anywhere in the disclosure as originally filed, to support these new elements.

Specifically the newly added Figure 5 appears to be an attempt to provide support for Applicant's argument that the vote serial number is assigned after a vote is cast (see figure below, emphasis added), as will be discussed in detail below, examiner finds no support for such an element/feature/limitation in the originally filed disclosure and therefore maintains that Figure 5, and all references to Figure 5, in the amendments to the Specification filed April 6, 2007 represent new matter and accordingly will not be entered.

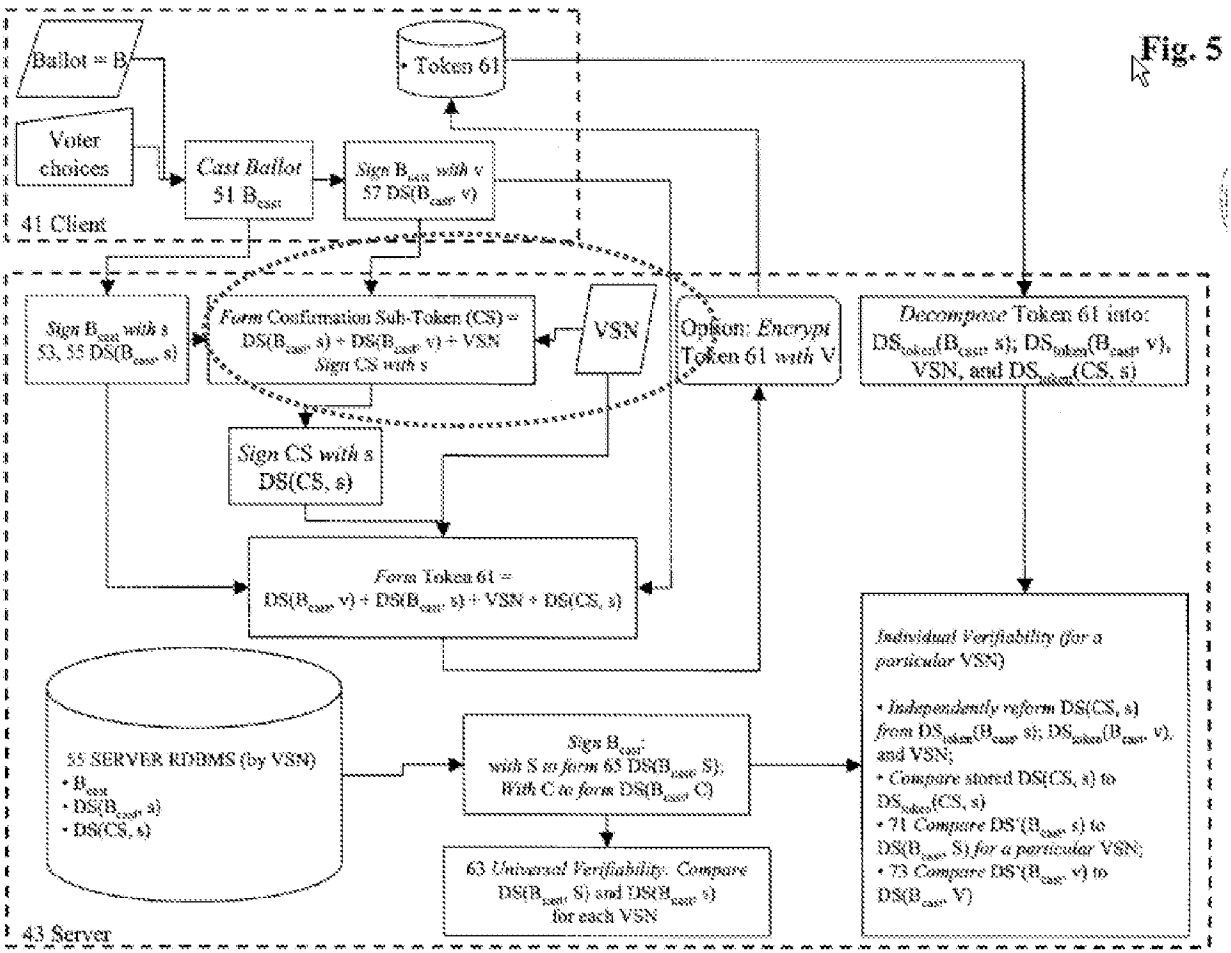

Fig. 5

b) In response to Applicant's argument that the amendments to the Specification filed April 6, 2007 the examiner agrees in part. Specifically examiner finds Applicant's argument that the deletion of unclaimed subject matter from the specification does not represent new matter (Last Paragraph, Page 7). However, the amendment to the Specification will not be entered since the amendment includes reference(s) to Figure 5 which will not be entered and therefore not presently in the disclosure (see Paragraph 0032).

In support of their argument and for the new matter Applicants state that Paragraphs 0054, 0070 and Figures 2, 3 disclose when and how a vote serial number is assigned to a ballot (Paragraphs 2-3, Page 8), the examiner respectfully disagrees.

The originally filed disclosure recites the vote serial number in only the following Paragraphs 0018, 0023, 0054, 0057, 0070 and 0072 (some of which are reproduced below, emphasis added) of which Paragraphs 0018 and 0023 provide the most relevant details as to when and how a vote serial number is associated/assigned to a ballot (namely prior to the ballot being cast).

> [0018] In accordance with one aspect of the invention, there is provided *a method of securely voting over a network*, which can be a local area network, or a wide area network such as the global computer network known as the Internet. The method involves **delivering an electronic ballot from a server with a vote serial number on the ballot**, to an individual at a terminal over a connection secured using both the server's and the voter's private keys. **Thereafter, the ballot is filled in with the voter's choices**, which are digitally signed using the voter's private key. The voter's ballot choices, bearing the voter's electronic signature, and **the vote serial number is then delivered to the server**. A data element is then created from the individual's digital signature of the ballot choices, the server's digital signature of the voter's ballot choices (created using the server's private key) and the vote serial number to allow recording of the subset of the ballot in a data store at the server, and retaining the ballot information as a vote. This data element is then digitally signed using the server's private key to ensure its integrity and authenticity.

[0023] In an alternative aspect, there is described a system for conducting *secure voting over a network*, for example, the global computer network known as the Internet, or on a local area network. The system includes a server having a data store associated therewith. The server is configured for connection to the network for communicating with terminals connected to the network. The server is further configured for **delivering an electronic ballot having the vote serial number on the ballot,** to an individual at a terminal connected to the network, and th**e ballot being configured for being filled in by the individual,** and for having a subset thereof delivered to the server with the individual's electronic signature, and the vote serial number thereon.

[0054] The individual's signature of the ballot is then delivered to the server 43 side where it is combined with three other elements at block 59. Specifically, the server's signature 53 is combined with the individual's signature 57 along with **a vote serial number (VSN) which is, for example, like a ballot serial number and can be an *arbitrary number* that goes from one to infinity. The vote serial number can be *generated per election*, and has no relationship to the voter, and is just an incidental sequence number that indicates a vote delivered in the election.** Those three elements are then digitally signed by the server yielding DS(C,s), and the four combine into an aggregation of core components which is a ballot confirmation token. This allows confirmation that a particular ballot has been retained in the system and no tampering has occurred. That token is then transmitted back to the individual as a confirmation token 61. The confirmation token 61 can then be encrypted with the individual's public

[0070] It will be appreciated that within the collection 109 of function boxes, separate functionality and information is provided, for example, from the collection of election ballots 113, **vote serial numbers** 119, and certificates 117, characterized preferably as X.509 certificates. In the Figure, block 115 is typically the application database server 23 shown in FIG. 1 and serves to compile the election voter table, election database and optionally, a voter demographics database, all of which will be described hereafter with reference to the lower half of FIG. 3.

Should Applicant's submit a new amendment to the Specification without references to the non-entered Figure 5 and in line with the April 6, 2007 submission the examiner will consider entering it.

However, the examiner notes that if the applicant's submit revisions similar to those proposed for Paragraphs 0018 and 0023 the examiner request that Applicant's cite specific paragraphs and phrases within those paragraphs or specific Figure elements that support the revisions and more importantly that clearly define when and how the vote serial number is assigned to a ballot for without originally filed Paragraphs 0018 and 0023 Applicant's specification lacks any specificity or clarity as to how or when a vote serial number is assigned/associated to/with a ballot (i.e. the specification, if amended as proposed, would provide no guidance as to how to interpret the claim "associating the Bcast and DS(Bcast,s) with a vote serial number VSN").

Further examiner notes the timing of the proposed amendments to Paragraphs 0018 and 0023, specifically that the amendment was made following the October 5,

2006 and November 2, 2006 interviews with the examiner wherein the examiner and Applicant's representative discussed the specification's lack of support for associating/assigning of a vote serial number only after a ballot is cast and it's teachings against such a limitation; an excerpt from the November 2nd interview is provided below for the Applicant's convenience (emphasis added).

> Applicant's representative and examiner discussed several features that Mr. Dimino and Mr. Corrado felt distinguished the instant application, per discussions during the October 5, 2006 interview and applicant's remarks filed October 10, 2006, namely individual verifiability and the assignment of a vote serial number. The examiner performed a quick review of the prior art to demonstrate *why these features were unlikely to distinguish the instant application over the prior art*. Note: This is not a complete search, just an initial review to show that the features are well known.
>
> References teaching Individual Verifiability and Vote Serial Number:
>
> - Cranor et al., Design and Implementation of a Practical Security Conscious Electronic Polling System (1996), P 1-2, Pg 12, "receipt #", Fig 1, P3-4, Page 8, db index, P1, Pg 11
> - VoteHere.net We Pages (2000) P5, Pg 17, P3,6, Pg 9, Pg 13
> - Reardon US 6,968,999: C5 L55-68, Fig 2 E 23, 24; C3 L23-38, C5 L63-68, Fig 2 E23,24
> - Chung US 7,036,730: C7 L8-23, C8 L37-55, "voting session identifier", C2 L60-68, C3, L8-30, C5 L8-15, 56-58; C10 L35-45, Fig 4c

Applicant's representative and examiner further discussed that in the remarks filed October 10 *several of the features argued are not positively recited in the body of the claims*, specifically that the VSN has no relationship with the voter, voters validating their own ballot and that the verification message does not contain the actual votes from the ballot.

Applicant's representative and examiner discussed Paragraph 0018 of the specification which indicates that the *vote serial number is applied to the ballot prior to it being cast by the voter*, whereby the examiner was unable to find support for the applicant's suggestion that the vote serial number was only applied after the voter cast their ballot - "The method involves delivering an electronic ballot from a server with a vote serial number on the ballot, to an individual at a terminal over a connection secured using both the server's and the voter's private keys. Thereafter, the ballot is filled in with the voter's choices, which are digitally signed using the voter's private key. The voter's ballot choices, bearing the voter's electronic signature, and the vote serial number is then delivered to the server."

c) In response to Applicant's argument that the OA makes a mistake of fact in asserting that the original specification does not disclose individual verifiability, the examiner believes Applicant's have misinterpreted the point the examiner raised.

The examiner was simply pointing out that the proposed amendments to the specification would add steps related to individual verifiability which were not originally disclosed.

d) In response to the Applicant's argument that the recent OA mischaracterizes SHRADER and CRANOR with the effect that the claims as submitted by the applicant, have not yet been examined. Mischaracterized terms include "cast ballots," "vote serial number," and "user."; the examiner respectfully disagrees.

As an initial matter the examiner has given the terms cast ballot, vote serial number and user the usual and customary definitions (cast ballot: voted ballot, committed ballot, vote, completed ballot, submitted ballot, vote; vote serial number: any unique vote identifier). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Specifically, in response to the Applicant's argument that the OA mischaracterized the phrase "cast ballot" the examiner notes that the prior art of record clearly teaches voters casting (submitting) their ballots wherein the ballots (vote) contains their choices and further wherein those cast ballots are commonly protected by some a cryptographic function such as a digital signature, PKD encryption or the like (Shrader et al.: Paragraphs 0048-0053).

Shrader et al. teach a system and method for securely voting over a network wherein voters complete and submit (cast) their ballots (Paragraphs 0035, 0041, 0042, 0059-0060; Figure 4, Elements 44-45; Figure 7, Elements 66-67).

> "*Voting entity casts its votes and encrypts the votes and the electronic ballot* with the public key of the voting tabulator before sending the encrypted voting information to the voting tabulator.", emphasis added, Paragraph 0062

Cranor et al. teaches a system and method for securely voting over a network wherein users (voters) cast and sign (encrypting, sealing) their cast ballot (encrypted ballot; Paragraph 5, Page 7; Paragraph 3, Page 8; Figure 1, b - blinded ballot digest).

> Pollster The pollster acts as a voter's agent, presenting human readable ballots to a voter, *collecting the voter's responses to ballot questions*, *performing cryptographic functions* on the voter's behalf, obtaining necessary validations and *receipts, and delivering ballots to the ballot box*. (emphasis added, Paragraph 5, Page 7)

> Tallier The tallier is responsible for *collecting the voted ballots* and tallying the results of the election or survey. *Voters first submit encrypted ballots, signed by the validator to the tallier.* The tallier checks the authenticity of the validation and verifies that the *encrypted ballot is unique* among the encrypted ballots received thus far. If the ballot is valid and unique, the tallier *issues a signed receipt to the voter*. The voter then submits the ballot decryption key. The tallier uses the key to decrypt the ballot. After the election, the tallier publishes a list of encrypted ballots, decryption keys, and decrypted ballots, allowing for independent verification of election results. (emphasis added, Paragraph 3, Page 8)

In response to the Applicant's argument that the OA mischaracterized the phrase "vote serial number", as defined by the specification "Note that the VSN… is ***just an***

incidental sequence number that indicates a vote was delivered in the election" (emphasis added, Paragraph 0054), the examiner respectfully disagrees.

Shrader et al. teach a system and method for securely voting over a network wherein ballots, both cast and pre-cast, are assigned a vote serial number (unique identifier; Figure 6, Element 58; ballot number, Paragraph 0063;

> "creates a electronic ballot consisting of the unique election identification and *ballot serial number*", emphasis added, Paragraph 0061

Cranor et al., teaches a system and method for voting securely over a network comprising associating at least two unique identifiers to ballots cast by voters wherein the unique identifiers (vote serial numbers) are generated and associated with the cast ballot only *after* the voters casts their ballot containing their choices (receipt number: Paragraphs 3-4, Page 8; Figure 1; index number for uniquely identifying, accessing and storing cast ballots in a database, Paragraph 4, Page 8)

> Our tallier computes a 16-byte digest of *each encrypted ballot received* and uses it *to index the encrypted ballots and receipts*. A hash table could be added for greater efficiency in *looking up encrypted ballots*. This modification is probably necessary to accommodate large-scale elections. (emphasis added, Paragraph 4, Page 8)

e) In response to Applicant's argument that SHRADER discloses the wrong data, encrypted with the wrong key; the examiner respectfully disagrees.

Shrader et al. teach a method and system for assisting a user in verifying a cast ballot recorded (saved, stored, executed, etc.) in a system (server) comprising (Abstract; Paragraphs 0050-0053; 0060-0063; Figures 4-8) forming (generating, creating, signing, encrypting, etc.) a digital signature of a cast ballot using the private key of a system (server; "The voting tabulator *signs, encrypts and sends the encrypted electronic ballot* to the voting mediator 72 in a message that is encrypted with the voting mediator's public key and signed with the *validator's private key*; Paragraph 0063; Figures 7-8, Element 72); associating (storing, linking, relating, etc.) the cast ballot, the voter's digital signature of the ballot with a ballot number (vote serial number, unique number/unique identifier, etc.; validating ballot request; Paragraph 0061; Figures 5-6, Elements 57, 58; validating/authenticating cast ballot; Paragraph 0063; Figure 8, Element 71) and forming a message (confirmation, string, receipt, acknowledgement, token, etc.) comprising a system's digital signature of the ballot and the ballot number (verification message(s) exchanged between tabulator to mediator; Paragraphs 0061, 0063; Figures 7-8).

f) In response to the Applicant's argument that the OA mischaracterized the phrase "user" the examiner respectfully disagrees.

Shrader et al. teach a system and method for secure network voting wherein at least one of the system/method participants/users is a voter who casts a ballot (Paragraphs 0035, 0041, 0042, 0059-0060; Figure 4, Elements 44-45; Figure 7, Elements 66-67).

Cranor et al. teach a system and method for securely voting over a network wherein at least one of the system/method participants/users is a voter who casts a ballot (Paragraph 5, Page 7; Paragraph 3, Page 8; Figure 1).

Additionally it is noted that the invention as claimed merely recites "making a confirmation token available to *a user*" wherein the claim does not positively recite that the "a user" performs any of the method steps as claimed nor does the invention as claimed positively recite which user (the "a user" recited in the preamble or another user of the system) the token is made available to nor does the invention as claimed positively recite what entity (the "a user" in the preamble or some other entity/participant) actually retrieves/receives the now available confirmation token nor does the invention as claimed positively recite what entity performs the comparison to determine that the cast ballot is verified (the "a user" of the preamble or another method participant/entity).

g)/h) In response to Applicant's argument that the recent OA mischaracterizes SHRADER to find a claimed comparison and recent OA neglects to account for an element of the Confirmation Token; the examiner respectfully disagrees.

Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

Applicant's arguments do not comply with 37 CFR 1.111(c) because they do not clearly point out the patentable novelty which he or she thinks the claims present in view of the state of the art disclosed by the references cited or the objections made. Further, they do not show how the amendments avoid such references or objections.

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Examiner notes that in response to Applicant's request for an interview (Last Paragraph, Page 12), the examiner attempted to call Mr. Dimino several times during the week of January 7, 2008 and left at least one voicemail requesting Mr. Dimino call the examiner regarding this case. No response was received from Mr. Dimino.

Specification

5. The amendment filed April 6, 2007 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows: Paragraph 0032, reference to Figure 5.

Figure 5 introduces new matter wherein the examiner has been unable to find any support, in the paragraphs cited by the applicant's or in remainder of the disclosure as originally filed, to support these new elements.

Specifically the newly added Figure 5 appears to be an attempt to provide support for Applicant's argument that the vote serial number is assigned after a vote is cast (see figure above, emphasis added). Examiner finds no support for such an element/feature/limitation in the originally filed disclosure and therefore maintains that Figure 5, and all references to Figure 5, in the amendments to the Specification filed April 6, 2007 represent new matter and accordingly will not be entered.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 29-30 and 33 are rejected under 35 U.S.C. 102(e) as being anticipated by Shrader et al., U.S. Patent Publication No. 2002/0077887.

Regarding Claims 29 and 33 Shrader et al. teach a method and system for assisting a user in verifying a cast ballot recorded (saved, stored, executed, etc.) in a system (server) comprising (Abstract; Paragraphs 0050-0053; 0060-0063; Figures 4-8):

- forming (generating, creating, signing, encrypting, etc.) a digital signature of a cast ballot using the private key of a system (server; "The voting tabulator *signs, encrypts and sends the encrypted electronic ballot* to the voting mediator 72 in a message that is encrypted with the voting mediator's public key and signed with the *validator's private key*; Paragraph 0063; Figures 7-8, Element 72);

- associating (storing, linking, relating, etc.) the cast ballot, the voter's digital signature of the ballot with a ballot number (vote serial number, unique number/unique identifier, etc.; validating ballot request; Paragraph 0061; Figures 5-6, Elements 57, 58; validating/authenticating cast ballot; Paragraph 0063; Figure 8, Element 71);

- forming a message (confirmation, string, receipt, acknowledgement, token, etc.) comprising a system's digital signature of the ballot and the ballot number (verification message(s) exchanged between tabulator to mediator; Paragraphs 0061, 0063; Figures 7-8);

- making the message available (verification message exchanged between tabulator to mediator; Paragraphs 0061, 0063; Figures 7-8);

- receiving the message (verification message(s) exchanged between tabulator to mediator; Paragraphs 0061, 0063; Figures 7-8, Elements 72-74);

- extracting (decrypting, stripping, de-signing, deciphering, etc.) the ballot number and the system's digital signature from the message (verification message(s) exchanged between tabulator to mediator; Paragraph 0063; Figures 7-8, Elements 73-75);

- for vote serial number comparing the system's digital signature of the ballot received to the system's digital signature of the ballot (Paragraphs 0061-0063; Figures 7-8); and

- if the comparison shows equivalency (match, consistency, equality, etc.) determining that cast ballot (message, token, etc.) is verified (valid, authentic, genuine, unaltered, secure, etc.; Paragraphs 0061, 0063; Figures 7-8).

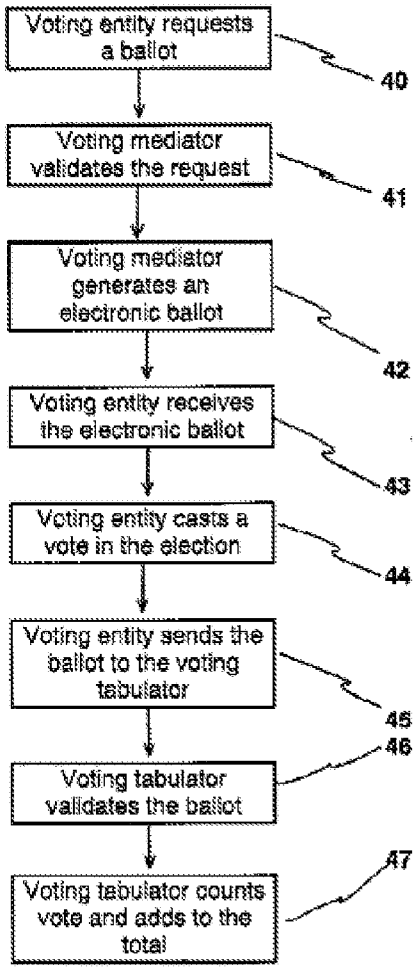
Voting entity requests a ballot
40
Voting mediator validates the request
41
Voting mediator generates an electronic ballot
42
Voting entity receives the electronic ballot
43
Voting entity casts a vote in the election
44
Voting entity sends the ballot to the voting tabulator
45
Voting tabulator validates the ballot
46
Voting tabulator counts vote and adds to the total
47

FIG. 4

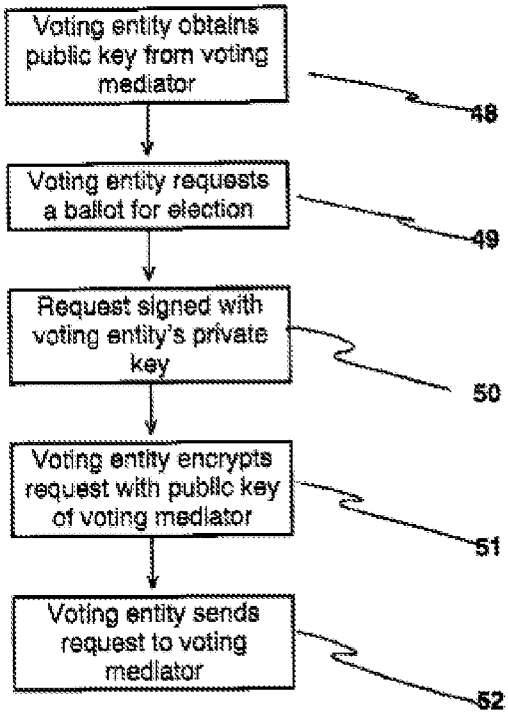
Voting entity obtains public key from voting mediator
48
Voting entity requests a ballot for election
49
Request signed with voting entity's private key
50
Voting entity encrypts request with public key of voting mediator
51
Voting entity sends request to voting mediator
52

FIG. 5

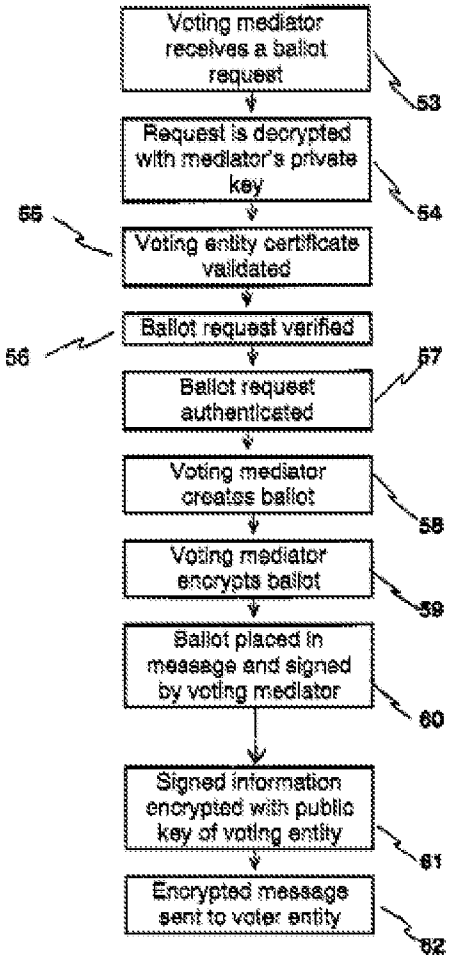
Voting mediator receives a ballot request
53
Request is decrypted with mediator's private key
54
55
Voting entity certificate validated
Ballot request verified
56
Ballot request authenticated
57
Voting mediator creates ballot
58
Voting mediator encrypts ballot
59
Ballot placed in message and signed by voting mediator
60
Signed information encrypted with public key of voting entity
61
Encrypted message sent to voter entity
62

FIG. 6

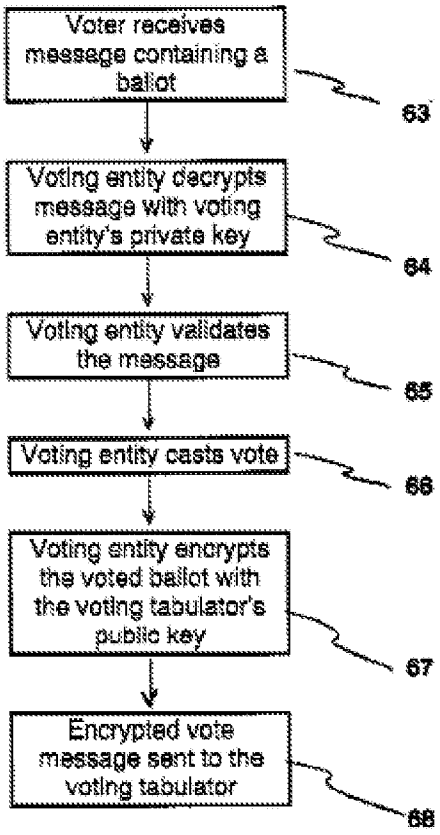
Voter receives message containing a ballot
63
Voting entity decrypts message with voting entity's private key
64
Voting entity validates the message
65
Voting entity casts vote
66
Voting entity encrypts the voted ballot with the voting tabulator's public key
67
Encrypted vote message sent to the voting tabulator
68

FIG. 7

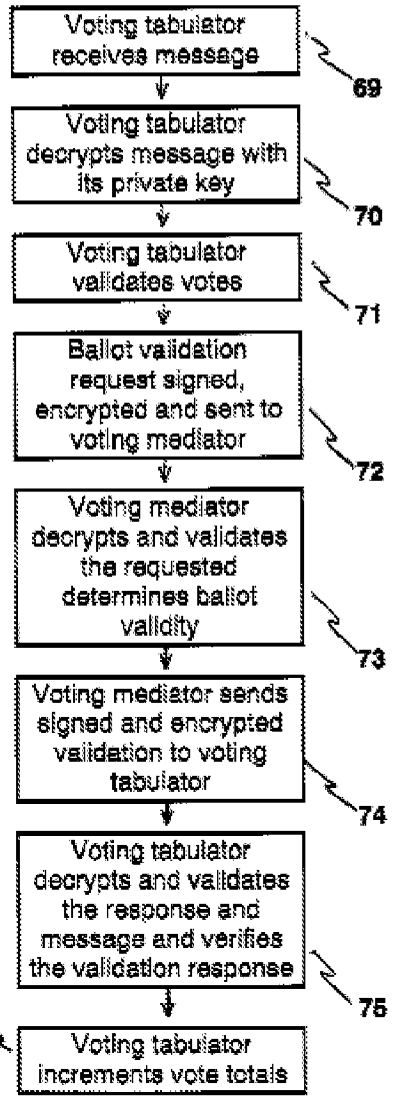

FIG. 8

Regarding Claim 30 Shrader et al. teach a method and system for assisting a user in verifying a ballot recorded in a system wherein the message (confirmation token, received token) further comprises the system's digital signature of the ballot and ballot number (aggregation; Paragraphs 0060-0062; Figure 2, Certificate No.); and wherein the method further comprises the steps of:

- extracting a digital signature of the ballot and ballot number (aggregation) from the message (received token; Paragraphs 0060, 0061, 0063; Figures 6-8); and

- the cast ballot is verified only upon the additional condition that the server's received digital signature of the aggregation is equivalent to the server's digital signature of the aggregation (Paragraphs 0061, 0063; Figures 6-8; Elements 67-75).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cranor et al., Design and Implementation of a Practical Security-Conscious Electronic Polling System (1996) in view of Shrader et al., U.S. Patent Publication No. 2002/0077887.

Regarding Claim 31 Cranor et al. teach a method and system for assisting a user in verifying (validating, authenticating, certifying, etc.) a cast ballot (vote) recorded (saved, stored, etc.) in a server (system) the method/system comprising (Abstract; Figures 1,3):

- receiving, in a system (server, computer, terminal, device, etc.), at least one set of a cast ballot and a voter's digital signature of the ballot (Paragraph 2, Page 5);

- forming (generating, creating, signing, encrypting, etc.) a digital signature of the ballot using the private key of a system (Paragraph 2, Page 5);

- associating (storing, linking, relating, etc.) the cast ballot, voter's digital signature of the ballot and the voter's identification number (Paragraphs 3-4, Page 7);

- forming a message (confirmation token, string, receipt, acknowledgement, etc.) comprising system's digital signature of the cast ballot, the voter's digital signature of the cast ballot, and the system's digital signature of the aggregation of the cast ballot, the voter's digital signature of the ballot and the system's digital signature of the ballot ("validator", "tallier", "validation certificate", "receipt"; Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1);

- making the message (token, string, etc.) available to a user (entity, voter, system, subsystem, third party, etc.; Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1);

- receiving the messages (confirmation, token, verification, acknowledgement, etc.; Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1);

- extracting (decrypting, stripping, etc.) *at least one of the following* from the message Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1):

  - voter's digital signature of the ballot; ***or***

  - system's digital signature of the ballot; ***or***

  - system's digital signature of the voter's digital signature of the ballot, the system's digital signature of the ballot, ballot number (aggregation);

- for extracted ballot number and the corresponding ballot number comparing *at least one of the following* (Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1):

- voter's digital signature of the ballot extracted from the message and voter's digital signature of the ballot; ***or***
- system's digital signature of the ballot extracted from the message and system's digital signature of the ballot, **or**
- system's digital signature of the ballot, digital signature of the voter's digital signature of the ballot, the system's digital signature of the ballot, ballot number (aggregation) extracted from the message and system's digital signature of the ballot, digital signature of the voter's digital signature of the ballot, the system's digital signature of the ballot, ballot number (aggregation); and

- if the comparison shows equivalency (match, consistency, equality, etc.) determining that the cast ballot is verified (valid, authentic, genuine, unaltered, accepted, counted, etc.; Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1).

Cranor et al. further teaches individual verifiability (Paragraphs 1-2, Page 12) as well as a unique vote/ballot identifier (receipt number/#; Figure 1, Pages 3-4; Page 8; db index, Paragraph 1, Page 11).

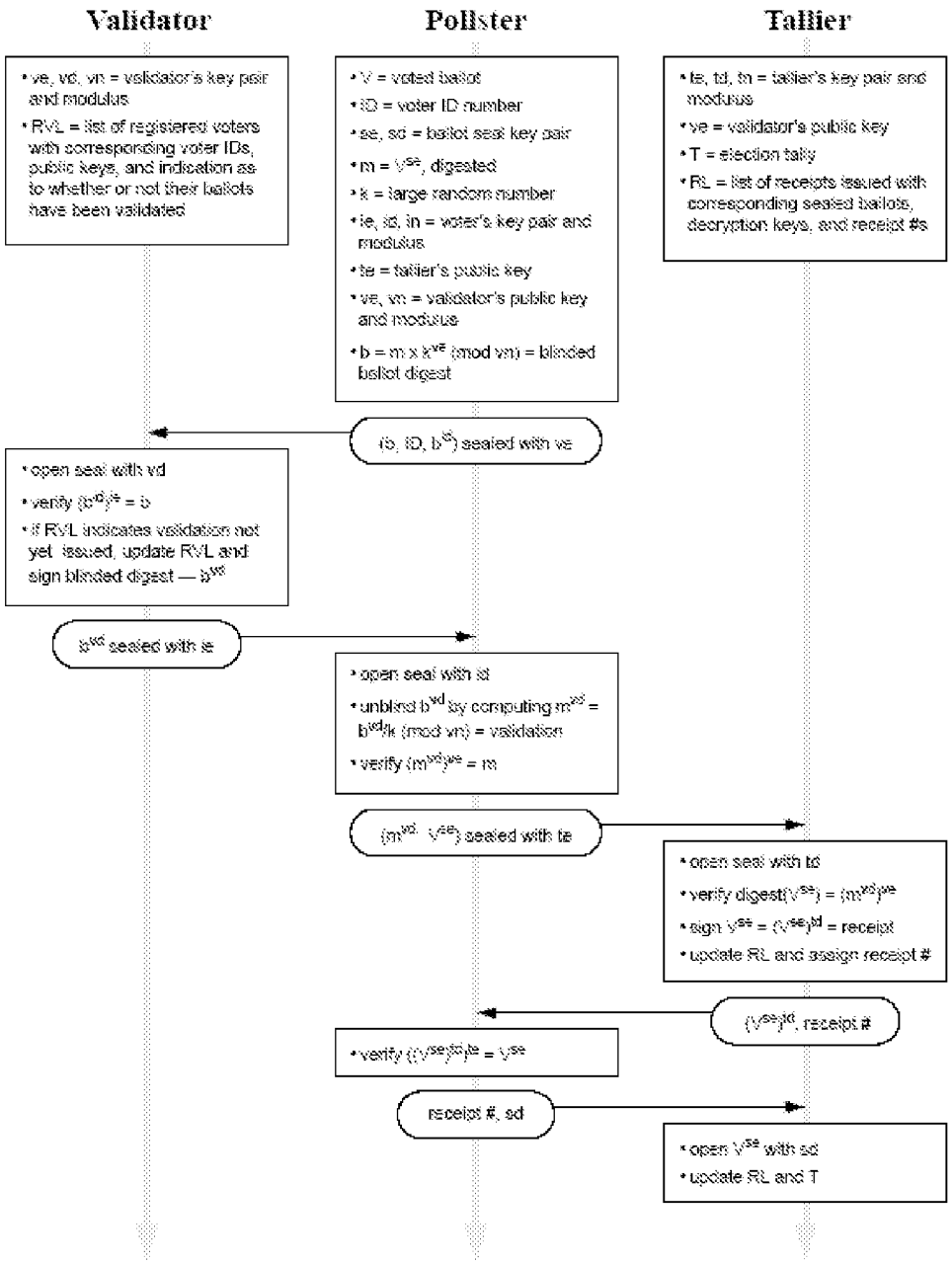

Figure 1: Blind Signature Protocol Overview

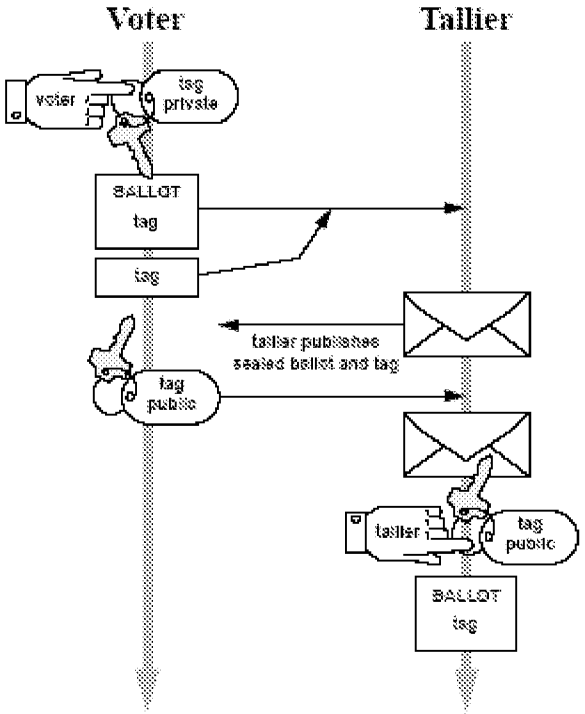

Figure 3: Phase 2 of the Two Agency Protocol

Cranor et al. teaches a system and method for voting securely over a network comprising *associating at least two unique identifiers with ballots cast by voters* wherein the unique identifiers (vote serial numbers) are generated and associated with the cast ballot only *after* the voters casts their ballot containing their choices (receipt number: Paragraphs 3-4, Page 8; Figure 1; index number for uniquely identifying, accessing and storing cast ballots in a database, Paragraph 4, Page 8)

Our tallier computes a 16-byte digest of *each encrypted ballot received* and uses it *to index the encrypted ballots and receipts*. A hash table could be added for greater efficiency in *looking up encrypted ballots*. This modification is probably necessary to accommodate large-scale elections. (emphasis added, Paragraph 4, Page 8)

While the use of unique identifiers for (paper and/or electronic) ballots is a common practice Cranor et al. does not expressly teach that the cast ballot contains a vote serial number as claimed.

Shrader et al. teach that ballots comprise a vote serial number (unique ballot ID, certificate no.) in an analogous art of secure electronic voting/balloting over a network for the purposes of ensuring voters only cast their ballot once (Paragraph 0061; Figures 2, 5-6, Elements 57, 58; validating/authenticating cast ballot; Paragraph 0063; Figure 8, Element 71).

It would have been obvious to one skilled in the art at the time of the invention that the system and method for verifying a cast ballot recorded on a system (server) as taught by Cranor et al. would have benefited from including in the ballot a unique ballot identifier (vote serial number) in view of the teachings of Shrader et al.; the resultant system/method providing an additional mechanism for ensuring that valid voters only vote once (Shrader et al.: Paragraph 0063).

Regarding Claim 32 Cranor et al. teach a method and system for verifying a cast ballot recorded in a system further comprising if the comparison shows equivalence between the system's digital signature of the ballot, digital signature of the voter's digital signature of the ballot, the system's digital signature of the ballot, extracted from the

message and system's digital signature of the ballot, digital signature of the voter's digital signature of the ballot and the system's digital signature of the ballot (aggregation) determining that the message (token) has not been modified (altered, disturbed, edited, etc.) since its formation (Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8).

Cranor et al. does not expressly teach that ballots further comprise vote serial numbers as claimed.

Shrader et al. teach that ballots comprise a vote serial number (unique ballot ID) in an analogous art of secure electronic voting/balloting for the purposes of ensuring voters only cast their ballot once (Paragraph 0061; Figures 5-6, Elements 57, 58; validating/authenticating cast ballot; Paragraph 0063; Figure 8, Element 71).

It would have been obvious to one skilled in the art at the time of the invention that the system and method for verifying a cast ballot recorded on a system (server) as taught by Cranor et al. would have benefited from including in the ballot a unique ballot identifier (vote serial number) in view of the teachings of Shrader et al.; the resultant system/method providing an additional mechanism for ensuring that valid voters only cast their ballot once (Shrader et al.: Paragraph 0063).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SCOTT L. JARRETT whose telephone number is (571)272-7033. The examiner can normally be reached on Monday-Friday, 8:00AM - 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hafiz Tariq can be reached on (571) 272-6729. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Scott L Jarrett/
Primary Examiner, Art Unit 3623